Perform System Administration
CAA2F103 / Version 1
01 Jun 2005

SECTION I. ADMINISTRATIVE DATA

All Courses Including This Lesson

Course Number	Version	Course Title
500-42A1O	1	Human Resources Specialist
500-42A3O	1	Human Resource Sergeant BNCOC
500-42F1O	1	Human Resources Information Systems Management Specialist
805C-42A30 (IDT)	1	Human Resource Specialist BNCOC
805C-42A30 (ADT)	2	Human Resource Sergeant BNCOC
805C-42A3O (ADT)	1	Human Resources Specialist BNCOC

Task(s) Taught(*) or Supported

Task Number	Task Title
	INDIVIDUAL
805C-42F-1210 (*)	Perform System Administration

Reinforced Task(s)

Task Number	Task Title

Academic Hours

The academic hours required to teach this lesson are as follows:

	Resident Hours/Methods
	1 hr 10 mins / Conference / Discussion
	5 hrs 30 mins / Demonstration
	1 hr 30 mins / Practical Exercise (Performance)
Test	1 hr
Test Review	30 mins
Total Hours:	10 hrs

Test Lesson Number

	Hours	Lesson No.
Testing (to include test review)		N/A

Prerequisite Lesson(s)

Lesson Number	Lesson Title
CAA2FS01	INTRODUCTION TO eMILPO

Clearance Access

Security Level: Unclassified
Requirements: There are no clearance or access requirements for the lesson.

Foreign Disclosure Restrictions

FD5. This product/publication has been reviewed by the product developers in coordination with the Fort Jackson foreign disclosure authority. This product is releasable to students from all requesting foreign countries without restrictions.

References

Number	Title	Date	Additional Information
EMILPO FUNCTIONAL GUIDE	Electronic Military Personnel Office Functional Guidance	20 Apr 2005	
EMILPO USERS MANUAL	Electronic Military Personnel Office Users Manual	16 Mar 2005	

Student Study Assignments

None.

Instructor Requirements

Instructor must be familiar with this lesson and have a general knowledge of eMILPO.

Additional Support Personnel Requirements

Name	Stu Ratio	Qty	Man Hours
None			

Equipment Required for Instruction

Id Name	Stu Ratio	Instr Ratio	Spt	Qty	Exp
673000PROJECO Overhead Projector, Semi-Portable	1:16	1:1	No	1	No
673000SCREENW Screen, Projection Wall/Ceiling Mount or Portable	1:16	1:1	No	1	No
7020-00-000-0001 Computer Workstation	1:1	1:1	No	17	No
7021-00-000-0003 Computer Server	1:16	1:1	No	1	No
702500BOARD Dry Erase/White Board	1:16	1:1	No	1	No
702500PRINTERLB Computer, Printer Laser (Black w/printer cable)	1:8	1:1	No	3	No
702500SURGE Surge Protector (Power Strip)	1:1	1:1	No	17	Yes

* Before Id indicates a TADSS

Materials Required

Instructor Materials:
Lesson Plan, Practical Exercise.

Student Materials:

Classroom, Training Area, and Range Requirements

Computer Classroom, 16 Positions

Ammunition Requirements

Id	Name	Exp	Stu Ratio	Instr Ratio	Spt Qty
None					

Instructional Guidance

NOTE: Before presenting this lesson, instructors must thoroughly prepare by studying this lesson and identified reference material.

Proponent Lesson Plan Approvals

Name	Rank	Position	Date
McCartney, Howard	SSG	Writer Developer	01 Jan 1900
Surls, Fredrick	GS-9	Writer Developer	01 Jan 1900
Burruss, Susan	GS-11	Team Chief	01 Jan 1900
Postoloff, Jon	GS-11	Information Sys Spec	01 Jan 1900
Jones, Anita	GS-13	Chief, TDD	01 Jan 1900
Knighton, Christine	COL		01 Jan 1900

SECTION II. INTRODUCTION

Method of Instruction: Conference / Discussion
Instructor to Student Ratio is: 1:10
Time of Instruction: 5 mins
Media: Programmed Instruction

Motivator

The Army is not any different from the civilian world in that there is always something going on behind the scene when computers are the main source of data information. Some one is responsible for creating, maintaining, and monitoring all users activity. You as the System Administrator (SA) will be responsible for establishing accounts for all users of eMILPO assigned to your installation. All commanders will look to you as the SA to maintain their individual clerks accounts and that the accounts are accessible at all times to maintain unit readiness. This is a great responsibility.

Terminal Learning Objective

NOTE: Inform the students of the following Terminal Learning Objective requirements.

At the completion of this lesson, you [the student] will:

Action:	Perform System Administration
Conditions:	Given a list of Unit Identification Codes (UIC), user names, eMILPO Access Request Forms, and access to a personal computer with eMILPO Portal available.
Standards:	1. Accessed the AHRS Portal. 2. Performed User Account Functions. 3. Performed System Functions. 4. Created System Reports.

Safety Requirements

All personnel with access to eMILPO equipment are responsible for the safety, proper use, normal care, and maintenance of such equipment.

No food or drink is allowed near or around electrical equipment (CPU, file servers, printer, projectors, etc.) due to possible elecrical shock or damage to equipment. Exercise care in personal movement in and through such areas. Avoid all electrical cords and associated wiring. In event of electrical storms, you will be instructed to power down equipment.

Risk Assessment Level

Low - None

Environmental Considerations

NOTE: It is the responsibility of all Soldiers and DA civilians to protect the environment from damage.

Evaluation

You will be given one practical exercise before the conclusion of the lesson and a one-hour test consisting of 10 questions after the lesson is completed.

Instructional

Lead-In

In this lesson, you will learn how to establish user accounts, remove user accounts, review maintenance procedures and system security requirements.

SECTION III. PRESENTATION

1. Learning Step / Activity 1. The AHRS Web Portal

Method of Instruction: Demonstration
Instructor to Student Ratio: 1:16
Time of Instruction: 1 hr 10 mins
Media: Programmed Instruction

Note to Instructor: Show PPT Slide #1 (Terminal Learning Objective).

Note: Ensure all students have an AKO user account before you proceed.

a. The eMILPO Web site is a secure site. Commanders at all echelons are responsible for designating individuals under their command who may be granted access to the eMILPO application. The AKO Web site will be the portal to the eMILPO application. All users requesting access to eMILPO must have an AKO user ID and password.

b. AKO User Registration. Students may obtain access to the AKO portal as follows:

1. To apply for an AKO User ID and Password, navigate to the AKO Web site at: www.us.army.mil.

2. Select the "I'm a New User" link, answer the appropriate security notices, and follow the onscreen instructions to fill out and submit a User Registration request.

3. Once the registration form and password have been submitted, AKO will inform you via email when the account has been approved and activated.

c. Access the AHRS Web Portal web site at https://emilpo.ahrs.army.mil.

Note to Instructor: Show PPT Slide #2 (AKO Authentication).

d. A window will appear requesting an Army Knowledge On-line (AKO) authentication. Enter an AKO User ID and Password and click the OK button.

Note to Instructor: Show PPT Slide #3 (AHRS Web Portal Applications menu).

e. This Web Portal gives you access to several different hyperlinks, the eMILPO hyperlink will be used for this lesson.

Note to Instructor: Show PPT Slide #4 (DoD Security Statement).

1. Upon clicking the eMILPO hyperlink on the AHRS Web Portal page, you will be prompted to view a standard DoD Security Statement acknowledging the level of security involved in accessing a DoD application.

2. To complete the security statement, perform the following steps:

(a) Click **Accept** to proceed to the eMILPO login authentication.

(b) Click **Decline** if you do not wish to acknowledge the security statement. The system will return you to the AHRS Web Portal page.

Note to Instructor: Show PPT Slide #5 (eMILPO login Authentication).

3. If you have selected to accept the DoD Security Statement, the system will present the eMILPO login authentication window. You will be prompted to enter your AKO credentials to enter eMILPO.

Note to Instructor: Show PPT Slide #6 (User Registration).

4. If you are a first-time eMILPO user, complete the eMILPO Access Request form and obtain the signature of your leader, manager, or supervisor before submitting the form to the System Administrator (SA) for your unit. The System Administrator will approve or deny access based on eMILPO security requirements. Only those users with the appropriate command authorizations, based on job and mission requirements with a need-to-know, will be given access.

f. Security. The eMILPO Web site is a secure site. Commanders at all echelons are responsible for designating individuals under their command who may be granted access to the eMILPO application. The AKO Web site will be the portal to the eMILPO application. All users requesting access to eMILPO must have an AKO user ID and Password.

1. All eMILPO/Datastore users granted access to the system, will follow the guidelines below:

(a) Ensure that all users have their own individual account. A user should never allow anyone to use his or her account.

(b) Users will be educated on the need to protect passwords.

Note: According to their units security Standard Operating Procedures (SOP).

(c) Passwords will not be transmitted through electronic mail (email).

(d) Password Protection - The following guidelines will be followed to protect system passwords.

-1- Passwords must never be written down or otherwise stored in a readable form. Knowledge of an individual's password must be limited to the user. Passwords must not be shared among users.

-2- It is everyone’s responsibility to report any suspected security violations immediately. When an individual user receives their password, they are acknowledging that they understand and accept all responsibilities associated with access to the eMILPO/Enterprise Datastore Systems.

NOTE: Conduct a check on learning and summarize the learning activity.

Q. What is the web site for eMILPO?
A. AHRS Web Portal is at https://emilpo.ahrs.army.mil.

Q. All users must have what type of User ID and password before request access to the AHRS Web Portal?
A. AKO User ID and password.

Q. How many users will share your account?
A. No users will share your account, accounts are issue to an individual.

Summary: During this learning activity we discussed gaining access to the Web Portal, registering with AKO, and security of the system.

2. Learning Step / Activity 2. eMILPO Access Request Form

Method of Instruction:	Demonstration
Instructor to Student Ratio:	1:16
Time of Instruction:	2 hrs 10 mins
Media:	Programmed Instruction

Note: Inform the student that this is the first step in granting a user account. You must have a completed eMILPO access request form on the individual requesting an account.

Note To Instructor: Show PPT Slide #7 (eMILPO Access Request Form).

a. Requests for eMILPO accounts are sent from the supervisor to the unit's User Administrator (UA) at the Personnel Automation Branch.

b. The UA will review the eMILPO Access Request Form sent from the unit supervisor. This form is vital to granting user accounts and access control.

c. The eMILPO Access Request Form is used for new accounts, modifications, and the removal of existing accounts.

1. **User Information**. Section one requires personal data about the User - user name, AKO user ID, e-mail address, social security number, contact phone number, rank, and primary grade. These blocks are all self-explanatory.

2. **Unit Profile Information**. The next section is the Unit Profile Information section – The UA uses this information to create the Unit Identification Code (UIC) hierarchy associated with each user. The information required for this section is the Associated UIC(s), which includes all UIC (s) that the user is responsible for maintaining. The User Role (optional), refers to the system users, administrators, and the permissions they will have that are defined within their user templates.

Note: Explain to the students that users may be associated with up to 15 UICs, and that a Start and End Date is required in the Unit Profile Information for security purposes. We will discuss associated UICs more in depth later in the lesson.

3. A distinction is made between functional roles and workflow roles within the eMILPO application. Functional roles refer to system users and administrators and the permissions they have that are defined within their user templates. User roles within eMILPO include the following:

(a) **Senior User Administrator (SUA)** – The SUA's responsibilities include the creation and management of groups and the rights associated with those groups. The SUA can create the following user accounts: SUA, User Administrator, and User. The SUA role will be performed by HQDA personnel.

(b) **User Administrator (UA)** – The UA's responsibilities include the creation and management of user accounts and user profiles, the assignment of groups to a user, and the locking/unlocking of user accounts. The UA may temporarily delegate a user role for the receipt of Workflow Notices (for

example, to cover for a period of vacation). The UA can also manage the Army's organizational hierarchy and turn workflow privileges on and off (for Slotting only) for units within his or her authorization.

(c) **Users** – This refers to the clerks who access the various personnel functions within the application. Their permissions are defined by the groups to which they are assigned.

4. **Supervisor/Leader/Manager Information**. This section requires the name and phone number of soldier's Supervisor/Leader/Manager.

5. **Requested Functions**. This section designates the required functions the users will be authorized to perform. The requester will check all the blocks that apply to their day-to-day performance. This is an overview of the eMILPO main menu. Ever block that is checked will be a highlighted function when the user logs into eMILPO. Requested functions can be selected by categories or areas.

6. **System Administration Information**. The System Administration Information section requires the name, signature, and date to be filled out by the approving UA.

Note: Inform the students that once the accounts have been granted the UA will notify the supervisor of the Soldier.

NOTE: Conduct a check on learning and summarize the learning activity.

Q. What type of is need to grant access to eMILPO?
A. An AKO user account and password and access to the internet.

Q. What does the user role establish?
A. The level of access privileges to the system for the workflow processing .

Q. What is an associated UIC?
A. Indicates the UIC that the user is associated with during an eMILPO session. Associate UIC gives the user access to specific unit data, and allows user to process varies transactions for personnel assigned to the UIC.

Summary: During this learning activity, we discussed the data required to gain access to the eMILPO Web Portal.

3. Learning Step / Activity 3. Establishing Users Accounts

Method of Instruction:	Demonstration
Instructor to Student Ratio:	1:16
Time of Instruction:	2 hrs 10 mins
Media:	Programmed Instruction

Note to Instructor: Show PPT Slide #8 (System Administration Menu).

a. The System Administration module allows the authorized User Administrator (UA) to perform unit hierarchy and user account management functions within eMILPO.

Note to Instructor: Show PPT Slide #9 (System Administration Menu eMILPO Screen)

b. The System Administration Menu allows the authorized UA to select an option to process system administration functions. The functions covered in this learning activity will be the User Account Functions, Group Functions, System Functions, and System Reports.

1. To access the functions available on the System Administration Menu, perform the following steps:

(a) **User Account Functions** - To perform User Account Functions, enter the user's AKO ID in the provided text entry field, and click on the corresponding radio button for the function.

(b) **Group Functions** -To perform a Group Function, enter a UIC in the provided text entry field, and click on the corresponding radio button for the function.

(c) **System Functions** -To perform System Function, enter a UIC in the provided text entry field, and click on the corresponding radio button for the function.

(d) **System Reports** -To generate a System Report, click on the corresponding radio button for there report.

(e) Click submit to proceed. The system will display the appropriate data page for the selected function.

c. Roles and Responsibilities. Remember, a distinction is made between functional roles (Senior User Administrator, User Administrator, and Users), and workflow roles within the eMILPO application. Workflow roles refer to the responsibilities of assigning tasks and approving personnel requests and actions. Workflow roles include the following:

1. Brigade S1 Chiefs and Clerks.
2. Battalion S1 Chiefs and Clerks.
3. Career Counselors.
4. Commanding Officers.
5. PERSTEMPO Chiefs and Clerks.
6. Human Resource Chiefs and Clerks
7. Senior System Administrators.
8. System Administrators.
9. Unit Administrators.
10. None.

Note: Explain the following system administration rules to the students.

1. **The UA will approve or deny requests for access based on eMILPO security requirements. Only those users with a legitimate reason to access the eMILPO application will be approved.**

2. **Only the UA can add, modify, remove, and unlock user access and accounts.**

3. **An UA can only add, modify, remove, and unlock user access or accounts for UICs for which he or she is authorized. The UA will not have visibility of user accounts with UICs that are not under his or her assigned authority.**

4. **A User's rights are determined by the Groups to which he or she has been assigned.**

Note to Instructor: Show PPT Slide #10 (User Account Functions).

d. User Account Functions. User Account Functions on the System Administration Menu, allow the UA to create, maintain, and remove user accounts for the unit boundaries that he or she is authorized to manage. All User Account Functions require that the UA provide an AKO User ID. Some User Account Functions will further require the UA to select an Associated UIC, if the user is associated with more than one UIC.

Note to Instructor: Explain to the students that at the Select Associated UIC screen they will type in the UIC for the account they wish to make changes too.

1. To access User Account Functions, the UA performs the following steps:

(a) From the System Administration Menu, Provide an AKO User ID for the user.

(b) Select an option by clicking the corresponding radio button.

(c) Click Submit to proceed. The system will authenticate the user ID to ensure it is a valid and active AKO User ID. The system will then display the appropriate page for processing.

(d) Click the Close to exit without proceeding. The system will return the UA to the Main Menu.

Note to Instructor: Show PPT Slide #11 (Add User Account Unit Profile).

2. To add a User, the UA performs the following steps:

(a) Under the subheading of User Information, the system displays the user data as currently recorded in the database as read-only. The captured information (Name, SSN, User ID, e-Mail Address, Phone Number, Rank, and P-Grade) is based on the entered AKO User ID.

(b) Under the User Information subheading, select a Workflow role from the Workflow Role pick-list. This is a required field. If a Workflow role is not applicable, select None.

(c) Under the User Information subheading, select the User role from the User Role pick-list. This is a required field.

(d) Under the subheading of Unit Profile Information:

Enter the Associated UIC as provided in the Access Request Form. This is a required field.

Enter a required Start Date for the account in the provided text-entry field.

Enter a required End Date for the account in the provided text-entry field.

(e) Under the subheading of Supervisor/Leader/Manager Information:

Enter the required Name of the manager who approved the Access Request Form.

Enter the required Phone Number in the provided text-entry field.

(f) Under the subheading of Access Control Information, indicate the type or level of access control for the user by checking on the corresponding radio button.

Unit Template—The user will inherit the access control template of the associated UIC. The UA will not need to assign access control for this user.

User Specific—The UA will assign a more specific or customized access control template for the user.

(g) Click Submit to proceed. The system will validate entry and display the Add User Group Control page, if the selection of User Specific was made. Otherwise, the system returns the user to the System Administration Menu. You can also Click Reset to clear all text-entry fields and start over, or Click Close to exit the page without saving. The system will return you to the System Administration Menu page.

Note to Instructor: Re-show PPT Slide #10 (User Account Functions), and explain that by selecting the corresponding radio button the student can choose another function.

Note to Instructor: Show PPT Slide #12 (Add User Access Control).

3. To add User Access Control, the UA performs the following steps:

(a) At the Add User Access Control page, you may select the functions you want to assign to the user from the Available Functions – Groups on the right. Select the functions you want to assign and click ADD. To select one functional area, click on the item. To select multiple functional areas that are in succession of each other, click on the first item, hold down the **Shift** key. To select multiple functional areas that are not in succession of each other, click on the first item, hold down the **Ctrl** key and click each succeeding item. The system adds the functions to the users Assigned Functions – Groups listing.

(b) Under Access Control at Sub-Unit(s), you may assign functions to the sub-units to which the user has rights. Select the function from the Available Functions – Groups and click Add. The functions will be added to the Assigned Functions – Groups.

(c) Click Submit to finish creating a user-specific user account. The system displays a message confirming that the user account has been created and asking if you would like to create another account. Click Yes to create another account; the system returns you to the System Administration Menu. Click No to return to the Main Menu.

(d) Click Close to return to the System Administration Menu without saving your changes. The system performs the following validations:

The system shall ensure that the entered AKO User ID is not already associated with the given Associated UIC.

The system shall ensure that the entered Associated UIC is within the unit boundaries of the UA. The UA cannot process account requests outside of his or her unit boundaries.

The system shall ensure that the unit profile data entered are valid.

Note to Instructor: Re-show PPT Slide #10 (User Account Functions), if need be.

4. The Modify User Account function allows the UA to make modifications to the unit profile and access control that were previously assigned to the user. To modify a user account, the UA performs the following steps:

(a) From the System Administration Menu, provide the AKO User ID for the user.

(b) Select the appropriate option by clicking the corresponding radio button.

(c) Click Submit to proceed. The system will authenticate the user ID to ensure that it is a valid and active AKO User ID before displaying the pertinent page.

Note to Instructor: Show PPT Slide #13 (Modify User Account Unit Profile)

5. To modify the Unit Profile for a User Account, the UA performs the following steps:

(a) The system displays the user data as currently recorded in the database as read-only.

(b) Under the Unit Profile Information – Associated UIC heading, the system displays the current values as recorded for the user unit profile. The UA may edit this data as necessary.

(c) Under the Supervisor/Leader/Manager Information heading, the system displays the current values as recorded for the user unit profile. The UA may edit these data as necessary.

(d) To change the Workflow Role for the user, perform the following steps:

Select a role from the Workflow Role pick-list.

Click Submit to proceed. The system validates the data entry and returns the UA to the System Administration Menu.

Click Close to exit the page without saving. The system returns the UA to the System Administration Menu for further processing.

(e) To change the User Role for the user from User to User Administrator, perform the following steps:

The system displays the Modify User Access – Group Control page.

Under Group Control at Associated Unit, select the Group you want to assign to the user from the Available Groups on the left and click Add. The Group will be added to the user's Assigned Groups on the right.

Click Submit to proceed. The system validates the data entry and returns the UA to the System Administration Menu.

Click Close to exit the page without saving. The system returns the UA to the System Administration Menu for further processing.

Note to Instructor: Show PPT Slide #14 (Modify User Account Access Control)

6. To modify the User Account Access Control, the UA performs the following steps:

(a) The system displays the user's data as currently recorded in the database as read-only. The system also displays the selected Associated UIC from the UIC Selection page as read-only.

(b) Under the subheading of Access Control at Associated Unit, the system populates the Available Functions – Groups with the functional categories and areas that exist in *e*MILPO. The UA may select one or more selections and click ADD to add to the current selections for the user.

(c) The system populates the Assigned Functions – Groups previously selected for the user. The UA may highlight one or more selections and click DEL to remove the functions.

(d) Under the subheading of Access Control at Sub-Units, the system populates the Available Functions – Groups with the functional categories and areas that exist in *e*MILPO. The UA may select one or more selections and click ADD to add to the current selections for the user.

(e) The system populates the Assigned Functions – Groups previously selected for the user. The UA may highlight one or more selections and click DEL to remove the functions.

(f) Click Submit to proceed. The system validates the data entry and returns the UA to the System Administration Menu.

(g) Click Close to exit the page without saving. The system returns the UA to the System Administration Menu.

Note to Instructor: Show PPT Slide #15 (Lock/Unlock User Account)

7. The Lock/Unlock User Account page allows the UA to lock an account and, therefore, make it inaccessible or unlock an account that has been previously locked. When the option is selected from the System Administration Menu, the system will determine if the entered AKO User ID is associated with more than one UIC. If the ID is associated with two UICs, the system will display the User Account—UIC Selection page so that one UIC can be selected. To lock or unlock a user account, the UA performs the following steps:

(a) Under the subheadings of User Information and Supervisor/Leader/Manager Information, the system displays the current data as read-only for verification purposes.

(b) Select the Lock or Unlock option by clicking on the corresponding radio button.

(c) Click Submit to proceed. The system will either lock or unlock the requested account. The system returns the UA to the System Administration Menu.

(d) Click Close to exit the page without proceeding. The system returns the UA to the System Administration Menu.

Note to Instructor: Show PPT Slide #16 (Remove User Account)

8. The Remove User Account function allows the authorized UA to remove an existing user account and remove *e*MILPO access for the selected user. When the option is selected from the System Administration Menu, the system will determine if

the entered AKO User ID is associated with more than one UIC. If the ID is associated with two UICs, the system will display the User Account—UIC Selection page so that one UIC can be selected. To remove a user account, the UA performs the following steps:

(a) Under the subheadings of User Information and Supervisor/Leader/Manager Information, the system displays the current data as read-only for verification purposes.

(b) Click Submit to proceed. The system will prompt the UA to confirm that the user's account and access to *e*MILPO for the Associated UIC is being removed. A Removal Confirmation Message, shows the message the UA receives to confirm removal of the user's account. Click Yes to continue.

9. The Delegate Workflow Role page allows the authorized UA to assign a workflow-related role from one user to another within his or her unit boundaries. Note: Explain to the students that Workflow Roles will be covered more in depth in a future lesson.

e. Group Functions. The Group Functions on the System Administration Menu allow the UA to view any Groups created in the eMILPO application as well as the functions assigned to that group.

f. System Functions. The System Functions on the System Administration Menu allow the UA to manage the hierarchy and access control templates of UICs within his or her unit boundaries. The UA also has the option to manage a unit's PSC status. All System Functions require that the UA provide an Associated UIC, and consist of the following actions:

1. The Modify Unit Hierarchy function allows the authorized UA to change the organizational hierarchy of a parent unit. Organizational hierarchy is defined as the administrative chain of command for a segment of the Army structure. Within the organizational hierarchy of units, a user will have access to his or her unit's data and those units that exist below it in the hierarchy. Users who are associated with a Personnel Service Center (PSC) will also have access to each of the units serviced by their PSC.

2. The Create/Modify Unit Access Control Template. The unit's access control template determines the data and functions that the unit and sub-units can access within eMILPO. The Create/Modify Unit Access Control Template page allows the authorized UA to revise a unit's access to data and functions.

3. The Personnel Service Center option allows the UA to assign a PSC to service a unit, designate a unit as a PSC, or remove the PSC designation from a unit.

g. System Reports. The System Reports option on the System Administration Menu allows the UA to view pertinent reports of UICs within his or her unit boundaries. The System Reports option offers the following reports:

1. Remove Inactive Accounts. The Remove Inactive Accounts report lists the user accounts that have been inactive for 30 day or greater and allows the authorized UA to remove those accounts.

2. Failed Logon Attempt Audit. The Failed Logon Attempt Audit report captures the failed attempts of logging in to eMILPO. These failed attempts are logged on the system for the purpose of inspection and action as necessary. This report allows the authorized UA to review and, if necessary, purge the audit records.

3. View Audit Report. The View Audit Reports option of the System Administration Menu allows the UA to view the actions that have been performed on eight major tables in the database. The View Audit Report (Filter Criteria Page), allows the UA to query the database for audit reports filtered by Table Name, Date Range, by SSN, or by AKO User ID. The eight tables are:

(a) Major Personnel Action Table

(b) Military Duty Status Table

(c) SFPA Table (Suspension of Favorable Personnel Actions)

(d) Soldier Table

(e) Soldier Lost Time Table

(f) Soldier Overseas Assignment Table

(g) Soldier Physical Qualification Table

(h) Soldier Rank Table

4. View Workflow Accounts. The View Workflow Accounts report displays all workflow accounts in the UA's unit hierarchy. The system displays the AKO User ID, UIC, Role, and SA Rights for all accounts as read-only.

NOTE: Conduct a check on learning and summarize the learning activity.

Q. What functions are accessed through the System Administration module?
A. ADD User Account, Modify User Account, Access Control and the Remove User Account.

Q. What type of account is required to access user account functions?
A. AKO.

Q. What is the purpose of the associated UIC field on the request access form?
A. The associated UIC field gives the user access to specific unit data, and allows the user to process various transactions for personnel assigned to the UIC.

Summary: During this lesson we covered the user account management functions in eMILPO. What are your questions?

4. Learning Step / Activity 4. Practical Exercise

Method of Instruction:	Practical Exercise (Performance)
Instructor to Student Ratio:	1:10
Time of Instruction:	1 hr 30 mins
Media:	Programmed Instruction

NOTE: Conduct a check on learning and summarize the learning activity.

5. Learning Step / Activity 5. Practical Exercise Review

Method of Instruction: Conference / Discussion
Instructor to Student Ratio: 1:10
Time of Instruction: 1 hr
Media: Programmed Instruction

NOTE: Conduct a check on learning and summarize the learning activity.

6. Learning Step / Activity 6. Test

Method of Instruction: Test
Instructor to Student Ratio: 1:10
Time of Instruction: 1 hr
Media: Programmed Instruction

NOTE: Conduct a check on learning and summarize the learning activity.

7. Learning Step / Activity 7. Test Review

Method of Instruction: Test Review
Instructor to Student Ratio: 1:10
Time of Instruction: 30 mins
Media: Programmed Instruction

NOTE: Conduct a check on learning and summarize the learning activity.

SECTION IV. SUMMARY

Method of Instruction: Conference / Discussion
Instructor to Student Ratio is: 1:10
Time of Instruction: 5 mins
Media: Programmed Instruction

Check on Learning

Determine if the students have learned the material presented by soliciting student questions and explanations. Ask the students questions and correct misunderstandings.

Review / Summarize Lesson

In this lesson, you were introduced to the System Administrator feature on eMILPO. Using this feature, you are able to add, modify, and remove User Account information.

SECTION V. STUDENT EVALUATION

Testing Requirements	**NOTE:** Describe how the student must demonstrate accomplishment of the TLO. Refer student to the Student Evaluation Plan.
Feedback Requirements	**NOTE:** Feedback is essential to effective learning. Schedule and provide feedback on the evaluation and any information to help answer students' questions about the test. Provide remedial training as needed.

Appendix A - Viewgraph Masters (N/A)

Appendix B - Test(s) and Test Solution(s) (N/A)

Appendix C - Practical Exercises and Solutions (N/A)

Appendix D - Student Handouts (N/A)